 <b>VERMONT</b> DEPARTMENT FOR CHILDREN AND FAMILIES <b>Family Services Policy Manual</b>		<h1>302</h1>
Chapter:	Federal Assurances	
Subject:	Criminal History Record Information (CHRI) Proper Access, Use, and Dissemination	Page 1 of 6
Approved:	Aryka Radke, Deputy Commissioner	Effective: 3/30/2023

## Purpose

To ensure the protection of the Criminal Justice Information (CJI) and its subset of Criminal History Record Information (CHRI) until such time as the information is purged or destroyed in accordance with applicable record retention rules.


## Table of Contents

Purpose .....	1
Table of Contents.....	1
Definitions .....	1
Policy .....	2
Proper Access, Use, and Dissemination of CHRI .....	2
Personnel Security Screening.....	3
Security Awareness Training.....	3
Physical Security.....	3
Media Protection .....	3
Media Transport.....	4
Media Sanitization and Disposal.....	4
Account Management.....	5
Remote Access .....	5
Personally Owned Information Systems.....	6
Reporting Information Security Events.....	6
Policy Violation and Misuse Notification.....	6

## Definitions

***Criminal Justice Information (CJI)***: The term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data.

***Criminal History Record Information (CHRI)***: A subset of CJI and for the purposes of this document is considered interchangeable. Due to its comparatively sensitive nature, additional controls are required for the access, use and dissemination of CHRI. In addition to the dissemination restrictions outlined below, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI.

 <b>VERMONT</b> DEPARTMENT FOR CHILDREN AND FAMILIES <b>Family Services Policy Manual</b>		<h1>302</h1>
Chapter:	Federal Assurances	
Subject:	Criminal History Record Information (CHRI) Proper Access, Use, and Dissemination	Page 2 of 6

***CJIS Systems Officer (CSO):*** The individual located within the CJIS Systems Agency responsible for the administration of the CJIS network on behalf of the CJIS Systems Agency. In Vermont this position is represented by the VT Department of Public Safety Vermont Crime Information Center Director.

***CJIS Systems Agency Information Security Officer (CSA ISO):*** The appointed FBI CJIS Division personnel responsible to coordinate information security efforts at all CJIS interface agencies.

***Information Security Officer (ISO):*** Typically, a member of an organization who has the responsibility to establish and maintain information security policy, assesses threats and vulnerabilities, performs risk and control assessments, oversees the governance of security operations, and establishes information security training awareness programs. The ISO also usually interfaces with security operations to manage implementation details and with auditors to verify compliance to established policies. In Vermont the ISO is represented by the VT Department of Public Safety Vermont Crime Information Center Assistant Director.


## Policy

This policy was developed using the FBI’s Criminal Justice Information Services (CJIS) and it shall always be the minimum standard for the division. The division’s policy stance may augment or increase the standards but shall not detract from the CJIS Security Policy standards.

The scope of this policy applies to any electronic or physical media containing FBI CJI while being stored, accessed, or physically moved from a secure location from the division. Additionally, this policy applies to any authorized person who accesses, stores, and/or transports electronic or physical media.

### **Proper Access, Use, and Dissemination of CHRI**

Information obtained from the Interstate Identification Index (III) is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, CFR. The III shall be accessed only for an authorized purpose. Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing noncriminal justice administrative functions on behalf of the authorized recipient and the outsourcing of said functions has been approved by appropriate CJIS Systems Agency (CSA) or State Identification Bureau

 <b>VERMONT</b> DEPARTMENT FOR CHILDREN AND FAMILIES <b>Family Services Policy Manual</b>		<h1>302</h1>
Chapter:	Federal Assurances	
Subject:	Criminal History Record Information (CHRI) Proper Access, Use, and Dissemination	Page 3 of 6

(SIB) officials with applicable agreements in place.

### **Personnel Security Screening**

Access to CJI and/or CHRI is restricted to authorized personnel. Authorized personnel are defined as an individual, or group of individuals, who have been appropriately vetted and have been granted access to CJI data. Agencies located within states having passed legislation authorizing or requiring civil fingerprint based background checks for personnel with access to CHRI for the purposes of licensing or employment shall submit fingerprint-based record check within 30 days of employment or assignment on all personnel with who have direct access to CJI, those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI, and any persons with access to physically secure locations or controlled areas containing CJI. Agencies located within states without this authorization or requirement are exempted from the fingerprint-based background check requirement until such time as appropriate legislation has been written into law.

### **Security Awareness Training**

Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI.


### **Physical Security**

A physically secure location is a facility or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect the FBI CJI and associated information systems. The perimeter of the physically secure location shall be prominently posted and separated from non-secure locations by physical controls.

Only authorized personnel will have access to physically secure non-public locations. The division will maintain and keep current a list of authorized personnel. All physical access points into the agency’s secure areas will be authorized before granting access. The agency will implement access controls and monitoring of physically secure areas for protecting all transmission and display mediums of CJI. Authorized personnel will take necessary steps to prevent and protect the agency from physical, logical and electronic breaches.

### **Media Protection**

Controls shall be in place to protect electronic and physical media containing CJI while at rest, stored, or actively being accessed. “Electronic media” includes memory devices

 <b>VERMONT</b> DEPARTMENT FOR CHILDREN AND FAMILIES <b>Family Services Policy Manual</b>		<h1>302</h1>
Chapter:	Federal Assurances	
Subject:	Criminal History Record Information (CHRI) Proper Access, Use, and Dissemination	Page 4 of 6

in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. “Physical media” includes printed documents and imagery that contain CJI.

The agency shall securely store electronic and physical media within physically secure locations or controlled areas. The agency shall restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per Section 5.10.1.2.

**Media Transport**

Controls shall be in place to protect electronic and physical media containing CJI while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. The agency shall protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

**Media Sanitization and Disposal**


When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, print-outs, and other similar items used to process, store and/or transmit FBI CJI shall be properly disposed of in accordance with measures established by the agency, department, and/or division.

Physical media (print-outs and other physical media) shall be disposed of by one of the following methods:

- 1) shredding using division issued shredders.
- 2) placed in locked shredding bins for a private contractor to come on-site and shred, witnessed division personnel throughout the entire process.
- 3) incineration using division incinerators or witnessed by division personnel onsite at agency or at contractor incineration site, if conducted by nonauthorized personnel.

Electronic media (hard-drives, tape cartridge, CDs, printer ribbons, flash drives, printer and copier Hard-drives, etc.) shall be disposed of by one of the methods:

- 1) Overwriting (at least 3 times) - an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located.

 <b>VERMONT</b> DEPARTMENT FOR CHILDREN AND FAMILIES <b>Family Services Policy Manual</b>		<h1>302</h1>
Chapter:	Federal Assurances	
Subject:	Criminal History Record Information (CHRI) Proper Access, Use, and Dissemination	Page 5 of 6

- 2) Degaussing - a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets (e.g., those used to hang a picture on a wall) are fairly weak and cannot effectively degauss magnetic media.
- 3) Destruction – a method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be pulled.

IT systems that have been used to process, store, or transmit FBI CJI and/or sensitive and classified information shall not be released from the division’s control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

### **Account Management**


The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate information system accounts at least annually and shall document the validation process.

All accounts shall be reviewed at least annually by the designated CJIS point of contact (POC) or his/her designee to ensure that access and account privileges commensurate with job functions, need-to-know, and employment status on systems that contain Criminal Justice Information. The POC may also conduct periodic reviews.

### **Remote Access**

The division shall authorize, monitor, and control all methods of remote access to the information systems that can access, process, transmit, and/or store FBI CJI. Remote access is any temporary access to an agency’s information system by a user (or an information system) communicating temporarily through an external, non-agency controlled network (e.g., the Internet).

The division shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The division shall control all remote accesses through managed access control points. The division may permit remote access for privileged functions only for compelling operational needs but shall document the rationale for such access in the security plan for the information system.

 <b>VERMONT</b> DEPARTMENT FOR CHILDREN AND FAMILIES <b>Family Services Policy Manual</b>		<h1>302</h1>
Chapter:	Federal Assurances	
Subject:	Criminal History Record Information (CHRI) Proper Access, Use, and Dissemination	Page 6 of 6

Utilizing publicly accessible computers to access, process, store or transmit CJJ is prohibited. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

### **Personally Owned Information Systems**

A personally owned information system shall not be authorized to access, process, store or transmit CJJ unless the agency has established and documented the specific terms and conditions for personally owned information system usage. A personal device includes any portable technology like camera, USB flash drives, USB thumb drives, DVDs, CDs, air cards and mobile wireless devices such as Androids, Blackberry OS, Apple iOS, Windows Mobile, Symbian, tablets, laptops or any personal desktop computer. When bring your own devices (BYOD) are authorized, they shall be controlled using the requirements in Section 5.13 of the CJIS Security Policy.

### **Reporting Information Security Events**

The agency shall promptly report incident information to appropriate authorities to include the state CSA or SIB's Information Security Officer (ISO). Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. ADS and Family Services Division leadership will be notified to help determine corrective action required. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

### **Policy Violation and Misuse Notification**

Violation of any of the requirements contained in the CJIS Security Policy or Title 28, Part 20, CFR, by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and/or termination.

Likewise, violation of any of the requirements contained in the CJIS Security Policy or Title 28, Part 20, CFR, by any visitor can result in similar disciplinary action against the sponsoring employee, and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.